Finite Fields and Their Applications 18 (2012) 437–444

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

The construction of replaceable $(q+3)$-nests of reguli in PG$(3,q)$

Alan R. Prince

Maxwell Institute for Mathematical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, Scotland, United Kingdom

ARTICLE INFO

Article history:
Received 11 July 2011
Revised 28 September 2011
Accepted 3 October 2011
Available online 10 October 2011
Communicated by Simeon Ball

MSC:
51E20
51A40
05B25

Keywords:
Inversive geometry
Nests of reguli
Translation planes
Spreads

ABSTRACT

We describe a construction of $(q+3)$-nests of reguli in PG$(3,q)$ for q odd, $q \geqslant 5$, and examine the replacement question. Two examples, a replaceable 10-nest in PG$(2,7)$ and a replaceable 14-nest in PG$(3,11)$, are of particular interest since there is no replacement set consisting of a union of opposite half-reguli. For all previously known examples of replaceable nests, there is a replacement set consisting of a union of opposite half-reguli.

1. Introduction

Throughout this paper, q is odd. Every translation plane of order q^n, with kernel containing GF(q), arises from a spread of PG$(2n-1,q)$. In particular, translation planes of order q^2, with kernel containing GF(q), arise from spreads of PG$(3,q)$. The translation planes are isomorphic if and only if the spreads are projectively equivalent. If U is a proper subset of the set of lines of a regular spread Ω of PG$(3,q)$ and $V \neq U$ is a set of pairwise skew lines covering precisely the same set of points as the lines of U, then $\Omega' = (\Omega \setminus U) \cup V$ is a spread of PG$(3,q)$ and we say that Ω' has been derived from Ω by *replacement*. An example of this process is replacing a set of disjoint reguli in a regular spread by their opposites to obtain a *subregular* spread. A *nest* of reguli in Ω is a set N of reguli

E-mail address: a.r.prince@ma.hw.ac.uk.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.10.001

in Ω such that each line of Ω is contained in precisely 0 or 2 reguli of N. If N contains k reguli, then N is called a k-nest and there are $k(q+1)/2$ distinct lines of Ω contained in the reguli of N. If U is the set of lines of a nest, then the nest is said to be *replaceable* if there is a replacement set $V \neq U$, as above. The concept of a nest of reguli was introduced by Baker and Ebert [1], generalising the notion of a Bruen *chain* of reguli [4]. Every Bruen chain is replaceable [9] but not every nest is. Replaceable nests have proved useful in constructing new spreads of PG$(3,q)$ and hence new translation planes. A *half-regulus* is any set of $(q+1)/2$ lines of a regulus. In all previously known examples of replaceable nests, there is a replacement partial spread V consisting of a union of half-reguli in the opposite reguli to the reguli of the nest. It has been proved that this must be the case for any replaceable k-nest with $k \leqslant q$ [12]. This raises the question of whether it must always be true (answered below).

In this paper, we generalise the construction in [6] to give a construction of $(q+3)$-nests in PG$(3,q)$ for q odd, $q \geqslant 5$. The line-set of each of these nests is a union of disjoint reguli so that the nests are replaceable by replacing some of these reguli by their opposites. We call such a replacement set *trivial*. The interesting question is whether there are *non-trivial* replacement sets. In two cases, a 10-nest in PG(3,7) and a 14-nest in PG(3,11), we find two different non-trivial replacement sets. A cyclotomic condition is given for the existence of these types of replacement set, in general, but it appears to be satisfied only in these two sporadic cases. The 10-nest in PG(3,7) and the 14-nest in PG(3,11) are of particular interest since there is no replacement partial spread consisting of a union of opposite half-reguli, thereby giving a negative answer to the question raised above.

2. Preliminary results

Bruck [3] showed that the lines and reguli of any regular spread of PG$(3,q)$ correspond to the points and circles of the Miquelian inversive plane $M(q)$ of order q. A model for $M(q)$ is obtained by taking its points to be the points of the projective line GF$(q^2) \cup \{\infty\}$ of order q^2 and its circles to be the projective sublines of order q. The circles not containing ∞ are the subsets $a + Hb = \{a + hb \mid h \in H\}$, $a, b \in \mathrm{GF}(q^2)$, $b \neq 0$, where H denotes the subgroup of GF$(q^2)^*$ of elements of norm 1 over GF(q). The circles containing ∞ are the subsets $\{a + bx \mid x \in \mathrm{GF}(q)\} \cup \{\infty\}$, $a, b \in \mathrm{GF}(q^2)$, $b \neq 0$. The multiplicative group of GF(q^2) acts on the circles by multiplication. If $a \neq 0$, the orbit of $a + Hb$ in this action contains the circle $1 + Hba^{-1}$.

The projective 3-space PG$(3,q)$ can be modelled using the vector space GF$(q^2) \oplus$ GF(q^2) over GF(q) (see [8]). Let L_∞ denote the line $\{(0,x) \mid x \in \mathrm{GF}(q^2)\}$. Then, the lines of PG$(3,q)$ disjoint to L_∞ are $[a,b] = \{(x, ax + bx^q) \mid x \in \mathrm{GF}(q^2)\}$ for $a, b \in \mathrm{GF}(q^2)$. The lines $[a,b]$ and $[c,d]$ intersect if and only if $a - c = (b - d)h$ for some element $h \in H$. The set of lines $\{[a,0] \mid a \in \mathrm{GF}(q^2)\} \cup \{L_\infty\}$ is a regular spread S of PG$(3,q)$. The correspondence $[a,0] \leftrightarrow a$ and $L_\infty \leftrightarrow \infty$ is the Bruck correspondence between the lines of S and the points of the projective line. The reguli not containing L_∞ are $[a + Hb, 0]$ and we have $[a + Hb, 0]' = [a, Hb]$, where R' denotes the opposite regulus to the regulus R (see [8, Lemma 2.2]). The lines other than L_∞ and $[0,0]$ can be partitioned into disjoint reguli $[Hb, 0]$, where b ranges over a set of distinct coset representatives of H in GF$(q^2)^*$.

Throughout the remainder of the paper, we assume that q is odd, $q \geqslant 5$, and fix the following notation: θ is a primitive element of GF(q^2), $\delta = \theta^{q-1}$, $H = \langle \delta \rangle$, $K = \mathrm{GF}(q)^*$. For $x \in \mathrm{GF}(q^2)$, $\bar{x}$ and $N(x)$ denote the conjugate and norm of x over GF(q) so that $\bar{x} = x^q$ and $N(x) = x^{q+1}$. Since $H \cap K = \{\pm 1\}$, HK has index 2 in GF$(q^2)^*$ and so consists of the squares of GF$(q^2)^*$. A coset Hb is called *even* if it contained in HK, otherwise it is called *odd*. An even coset Hb contains precisely 2 elements of K, which are negatives of each other, while an odd coset Hb does not contain any element of K. Note that, since HK is the set of all squares of GF$(q^2)^*$, Hb is even if and only if b is a square of GF$(q^2)^*$. The circle $a + Hb$ is called *even* if Hb is even, otherwise it is called *odd*. Observe that $\bar{\theta} = \delta\theta$, which implies that $\bar{\theta}^i = \delta^i \theta^i$. If $h \in H$, then $\bar{h} = h^{-1}$. The elements of the form $1 - h$ for $h \in H$ have some interesting properties. For example, $N(1-h) = (1-h)(1-\bar{h}) = 2 - h - \bar{h} = \mathrm{trace}(1-h)$ and $\overline{1-h} = 1 - h^{-1} = (1-h)(-h^{-1})$. We shall require the following version of [8, Lemma 3.3].

Lemma 2.1. *Any element of* $\mathrm{GF}(q^2)^*$*, not in* $\mathrm{GF}(q)^*$*, has a unique representation in the form* $(1-h_1)/(1-h_2)$*, where* h_1*,* h_2 *are distinct elements of* $H \setminus \{1\}$.

Proof. If $h_1, h_2 \in H \setminus \{1\}$ are distinct, then $(1-h_1)/(1-h_2)$ is not an element of $\mathrm{GF}(q)^*$ since its conjugate is $(h_2/h_1)(1-h_1)/(1-h_2)$. If $h_3, h_4 \in H \setminus \{1\}$ are distinct and $(1-h_1)/(1-h_2) = (1-h_3)/(1-h_4)$, then $(1-h_1)(1-h_4) = (1-h_2)(1-h_3)$. Taking conjugates gives $h_1h_4 = h_2h_3$ and expanding then gives $h_1+h_4 = h_2+h_3$. Thus, h_1, h_4 and h_2, h_3 are the roots of the same quadratic equation. Hence, $h_1 = h_3$ and $h_2 = h_4$. It follows that there are $q(q-1)$ distinct elements of the form $(1-h_1)/(1-h_2)$, where h_1, h_2 are distinct elements of $H \setminus \{1\}$. Thus, every element of $\mathrm{GF}(q^2)^*$, not in $\mathrm{GF}(q)^*$ can be written uniquely in this form. □

Lemma 2.2. *Suppose that* $\delta^s \neq -1$*. If* $1+\delta^s = \theta^t$*, then* $s+t \equiv 0 \bmod (q+1)$.

Proof. $\theta^{s+t} = \theta^s + \theta^s\delta^s = \mathrm{trace}(\theta^s) \in \mathrm{GF}(q)^*$. Hence, $s+t \equiv 0 \bmod (q+1)$. □

For the theory and terminology of finite geometries, inversive planes and finite fields, see [5] and [10].

3. The constructions

The following lemma describes the intersection pattern of the circle $1+Ha$ with the circles of the form Hb. As in [2], we say that $1+Ha$ is a *purely secant* circle if it is not tangent to any circle Hb (two circles are *tangent* or *secant* according as the number of points in common is 1 or 2, respectively). Since $1+Ha$ and Hb are distinct circles, $|(1+Ha) \cap Hb| = 0, 1, 2$. We remark that $|(1+Ha) \cap Hb| = (a,b)$, where (a,b) is defined to be the number of $x \in Ha$ such that $1+x \in Hb$. This cyclotomic number was first studied by H.H. Mitchell (see [11]).

Lemma 3.1.

(a) *If* $1+Ha$ *is tangent to* Hb*, then the point of tangency is an element of* $\mathrm{GF}(q)$ *and* $1+Ha$ *and* Hb *are even circles.*
(b) *If* $1+Ha$ *is an even circle, other than* $1+H$*, then* $1+Ha$ *is tangent to precisely two circles* Hb.
(c) *If* $1+Ha$ *is an odd circle, then* $1+Ha$ *is a purely secant circle.*
(d) *If* $1+Ha$ *is secant to* Hb*, then the two points of intersection are conjugate elements* $1+x$, $1+\bar{x}$ *of* $\mathrm{GF}(q^2)$*, where* $x, \bar{x} \in Ha$*. Moreover, the two points of intersection are in the same coset of* $H^{(2)} = \{h^2 \colon h \in H\}$ *if and only if* Hb *is an even circle.*

Proof. If $1+x$ is a common point of $1+Ha$ and Hb, where $x \in Ha$, then so is $1+\bar{x}$. Thus, if $1+Ha$ is tangent to Hb, then $x \in \mathrm{GF}(q)$ and $1+Ha$ and Hb are even circles. Moreover, the point of tangency is either $1+c$ or $1-c$, where $\pm c$ are the two elements of K in Ha. It follows that if $1+Ha$ is an even circle and $Ha \neq H$, then $1+Ha$ is tangent to precisely two circles Hb. The case $1+H$ is exceptional, since $1+H$ contains 0. If $1+Ha$ is an odd circle, then (a) implies that $1+Ha$ is not tangent to any circle Hb, proving (c). If $1+Ha$ is secant to Hb, then the points of intersection are distinct conjugate elements of $\mathrm{GF}(q^2)$ (the two elements of $\mathrm{GF}(q)$ in $1+Ha$, in the case that $1+Ha$ is even, are points of tangency). Thus, the two points of intersection are $y = 1+x$ and $\bar{y} = 1+\bar{x}$, where $x \in Ha$ and $1+x \in Hb$. If $y = \theta^i$, then $\bar{y} = \delta^i y$. Thus, y and $\bar{y}$ are in the same coset of $H^{(2)} = \{h^2 \colon h \in H\}$ if and only if i is even or, equivalently, y is a square of $\mathrm{GF}(q^2)^*$. Since y is a square of $\mathrm{GF}(q^2)^*$ if and only if its norm is a square of $\mathrm{GF}(q)^*$, this proves (d). □

Theorem 3.2.

(a) *If* $1+Ha$ *is an odd circle, then the reguli* $[h+Ha, 0]$ *for* $h \in H$ *form a* $(q+1)$*-nest.*
(b) *If* $1+Ha$ *is an even circle, other than* $1+H$*, then the reguli* $[h+Ha, 0]$ *for* $h \in H$*, together with the two reguli* $[Hb, 0]$ *corresponding to the circles* Hb *tangent to* $1+Ha$*, form a* $(q+3)$*-nest.*

Proof. (a) If $1 + Ha$ is an odd circle, then $1 + Ha$ is a purely secant circle by Lemma 3.1(c). Since multiplication by δ permutes the points of each circle Hb in a $(q+1)$-cycle, the circles in the H-orbit of $1 + Ha$ cover each of the points in the circles Hb secant to $1 + Ha$ twice (and only these points). Thus, since the H-orbit of $1 + Ha$ consists of the circles $h + Ha$ for $h \in H$, the corresponding reguli $[h + Ha, 0]$ form a $(q+1)$-nest.

(b) If $1 + Ha$ is an even circle, $Ha \neq H$, then $1 + Ha$ is tangent to precisely two circles Hb and secant to $(q-1)/2$ circles by Lemma 3.1(b). Consider the H-orbit of $1 + Ha$. Each point of the circles secant to $1 + Ha$ are covered twice by the circles of the orbit, whereas the points of the two tangent circles Hb are covered only once. By including the two tangent circles themselves, the resulting set of circles covers these points twice. Thus, the reguli corresponding to these circles, namely the reguli $[h + Ha, 0]$ for $h \in H$, together with the two reguli $[Hb, 0]$ corresponding to the tangent circles Hb, form a $(q+3)$-nest. □

Remark. (a) is essentially the construction of Ebert [6] but (b) is a new construction.

Lemma 3.3. *The circle $1 + Ha$ is secant, or tangent, to precisely the same circles Hb as the circle $a + H$.*

Proof. If $x \in Ha$, then $1 + x = x(1 + x^{-1})$. Thus, $N(1 + x) = N(x)N(1 + x^{-1}) = N(a)N(1 + x^{-1})$. As x ranges through the coset Ha, $1 + x$ ranges through the circle $1 + Ha$ and $a(1 + x^{-1})$ ranges through the circle $a(1 + Ha^{-1}) = a + H$. Since $1 + x$ and $a(1 + x^{-1})$ have the same norm, the lemma follows. □

4. The replacement question

Throughout this section, we assume that $1 + Ha \neq 1 + H$. The line-set of each of the nests constructed in Theorem 3.2 is a union of the disjoint reguli $[Hb, 0]$, where Hb ranges over the circles secant or tangent to $1 + Ha$. Thus, the nests are replaceable, by reversing some or all of these reguli to yield André spreads. We call such a replacement set *trivial*. The interesting question is whether there are *non-trivial* replacement sets. The H-orbit of $1 + Ha$ is the set of circles $\{h + Ha \mid h \in H\}$ with corresponding reguli $[h + Ha, 0]$. Denoting the regulus $[\delta^i + Ha, 0]$ by R_i, the corresponding reguli are $R_0, R_1, R_2, \ldots, R_q$.

The following lemma shows that the points of intersection of two circles $a_1 + Hb_1$ and $a_2 + Hb_2$ determine the intersections of the lines of the opposite reguli $[a_1, Hb_1]$ and $[a_2, Hb_2]$ and vice versa.

Lemma 4.1. *If $a_1 + h_1b_1 = a_2 + h_2b_2$ is a point of intersection of the circles $a_1 + Hb_1$ and $a_2 + Hb_2$, then the line $[a_1, hh_1b_1]$ of $[a_1, Hb_1]$ intersects the line $[a_2, hh_2b_2]$ of $[a_2, Hb_2]$ for each $h \in H$. Conversely, suppose that the line $[a_1, h_1b_1]$ of $[a_1, Hb_1]$ intersects the line $[a_2, h_2b_2]$ of $[a_2, Hb_2]$, then there exists $h \in H$ such that $a_1 + hh_1b_1 = a_2 + hh_2b_2$ is a point of intersection of the circles $a_1 + Hb_1$ and $a_2 + Hb_2$.*

Proof. This follows immediately from the fact that the line $[a, b]$ intersects the line $[c, d]$ if and only if there exists $h \in H$ such that $a - c = h(b - d)$. Note that if the line $[a, b]$ intersects the line $[c, d]$, then $[a, hb]$ intersects $[c, hd]$ for each $h \in H$. □

We now determine the intersections amongst the lines $[\delta^i, \delta^j a]$ of the opposite reguli $R'_0, R'_1, R'_2, \ldots, R'_q$. Note that the line $[\delta^i, \delta^j a]$ intersects the line $[\delta^k, \delta^l a]$ if and only if the line $[1, a]$ intersects the line $[\delta^{k-i}, \delta^{l-j} a]$. The following describes how the line $[1, a]$ of R'_0 intersects the lines of R'_i.

Lemma 4.2. *Suppose that $1 + \delta^i a$ and $1 + \delta^j a$ are conjugate elements of $1 + Ha$, so that $1 + \delta^i a = \delta^d(1 + \delta^j a)$ for some d. Then, the line $[1, a]$ of R'_0 intersects the line $[\delta^d, \delta^{d+j-i} a]$ of R'_d and the line $[\delta^{-d}, \delta^{-(d+j-i)} a]$ of R'_{-d}, where the subscript is interpreted modulo $(q+1)$. Conversely, any line of R'_d which intersects $[1, a]$*

corresponds in this way to some conjugate pair of elements $1+\delta^i a$ *and* $1+\delta^j a$ *such that* $1+\delta^i a = \delta^d(1+\delta^j a)$.

Proof. Since $1+\delta^i a = \delta^d + \delta^{d+j} a$, the line $[1, \delta^i a]$ of R'_0 intersects the line $[\delta^d, \delta^{d+j} a]$ of R'_d. Thus, the line $[1, a]$ of R'_0 intersects the line $[\delta^d, \delta^{d+j-i} a]$ of R'_d. Reversing the roles of $1+\delta^i a$ and $1+\delta^j a$: the line $[1, a]$ of R'_0 intersects the line $[\delta^{-d}, \delta^{-(d+j-i)} a]$ of R'_{-d}. □

The line $[\delta^i, \delta^j a]$ of R'_i is called *even* if j is even and *odd* if j is odd.

Lemma 4.3. *If* $1+Ha$ *is an odd circle, then the line* $[1, a]$ *of* R'_0 *intersects only odd lines of* R'_d *if* d *is even* ($d \neq 0$) *and intersects only even lines if* d *is odd. If* $1+Ha$ *is an even circle, then the line* $[1, a]$ *of* R'_0 *intersects only even lines of* R'_d *if* d *is even* ($d \neq 0$) *and intersects only odd lines if* d *is odd.*

(Note: $[1, a]$ does not intersect any of the lines of R'_d if R_0 and R_d are disjoint.)

Proof. Suppose that $1+\delta^i a$ and $1+\delta^j a$ are conjugate elements of $1+Ha$. Then, $\delta^i a$ and $\delta^j a$ are conjugate elements of Ha. Since $\delta^i a = \delta^{i-j}(\delta^j a)$ and $\overline{\theta^k} = \delta^k \theta^k$, we conclude that, if $1+Ha$ is an odd circle, then $i-j$ is odd, while if $1+Ha$ is an even circle, then $i-j$ is even. The theorem now follows from Lemma 4.2. □

Theorem 4.4. *If* $1+Ha$ *is an odd circle, then the even lines of* R'_d *for* d *even, together with the odd lines of* R'_d *for* d *odd, form a replacement partial spread for the* $(q+1)$*-nest* $R_0, R_1, \ldots, R_q$.

Proof. Since the line $[\delta^i, \delta^j a]$ intersects the line $[\delta^k, \delta^l a]$ if and only if the line $[1, a]$ intersects the line $[\delta^{k-i}, \delta^{l-j} a]$, this follows immediately Lemma 4.3. □

Theorem 4.4 shows that, in the purely secant case, there is a replacement set consisting of natural opposite half-reguli. This is proved also in [7]. Lemma 4.3 indicates that the situation is not so straightforward if $1+Ha$ is an even circle (the tangent case). In this case, we utilise Lemma 3.3 and consider the *companion* circle $a+H$. The H-orbit of $a+H$ is the set of circles $\{ha+H \mid h \in H\}$ for $h \in H$. The corresponding reguli are $S_0, S_1, \ldots, S_q$, where S_i denotes $[\delta^i a + H, 0]$. The opposite reguli are $S'_0, S'_1, \ldots, S'_q$, where $S'_i = [\delta^i a, H]$. We say that the line $[\delta^i a, \delta^j]$ of S'_i is *even* if j is even and *odd* if j is odd. The following describes how the line $[1, a]$ of R'_0 intersects the lines of S'_i.

Lemma 4.5. *If* $1+Ha$ *is an even circle, then the line* $[1, a]$ *of* R'_0 *intersects only even lines of* S'_d *if* d *is even and only odd lines if* d *is odd. If* $1+Ha$ *is an odd circle, then the line* $[1, a]$ *of* R'_0 *intersects one odd and one even line of* S'_d *for all* d.

Proof. The intersection of the circles $1+Ha$ and $ha+H$ is given by the solutions $x_1, x_2 \in H$ of the equation $1+x_1 a = ha + x_2$. The equation can be written in the form $ha(1-x_1/h) = 1-x_2$. There is a trivial solution $x_1 = h$, $x_2 = 1$. If $x_1 \neq h$ then $ha = (1-x_2)/(1-x_1/h)$ which gives a second solution $x_2 = h_1$, $x_1 = hh_2$ in the case that $ha \notin \mathrm{GF}(q)$, where h_1, h_2 are the uniquely determined nonidentity elements of H such that $ha = (1-h_1)/(1-h_2)$, given by Lemma 2.1. If $ha \in \mathrm{GF}(q)$, the trivial solution is the only one since ha has no representation as $(1-h_1)/(1-h_2)$. By Lemma 4.1, if $1+x_1 a = ha + x_2$, then $[1, a]$ intersects $[ha, x_2/x_1]$. Thus, if $ha \notin \mathrm{GF}(q)$, then the line $[1, a]$ intersects two lines of $[ha, H]$, namely $[ha, 1/h]$ and $[ha, h_1/h_2 h]$, where h_1, h_2 are the uniquely determined nonidentity elements of H such that $ha = (1-h_1)/(1-h_2)$. By Lemma 2.2, $1+h$ is a square of $\mathrm{GF}(q^2)^*$ if $h \in H^{(2)}$ and is a nonsquare otherwise. If $1+Ha$ is an even circle, then ha is a square of $\mathrm{GF}(q^2)^*$ and hence $h_1/h_2 \in H^{(2)}$. Thus, $1/h$ and $h_1/h_2 h$ are in the same coset of $H^{(2)}$. If $1+Ha$ is an odd circle, then ha is a nonsquare of $\mathrm{GF}(q^2)^*$ and hence $h_1/h_2 \notin H^{(2)}$. Thus, $1/h$ and $h_1/h_2 h$ are in opposite cosets of $H^{(2)}$. If $ha \in \mathrm{GF}(q)$, then the line $[1, a]$ intersects only one line of $[ha, H]$, namely

$[ha, 1/h]$. (This case can arise only if $1 + Ha$ is an even circle. Then, there are precisely two elements $ha \in \mathrm{GF}(q)$. Thus, in the tangent case, with two exceptions, $[1, a]$ intersects precisely two lines of $[ha, H]$.) □

In the case $q \equiv 3 \pmod 4$, we can refine Lemma 4.5. We define the *type* of the line $[\delta^i, \delta^j a]$ of R'_i and of the line $[\delta^i a, \delta^j]$ of S'_i to be the value of j mod 4. Thus, the even lines of S'_i are either type 0 or type 2 and the odd lines are either type 1 or type 3.

Lemma 4.6. *Assume that $q \equiv 3 \pmod 4$. If $1 + Ha$ is an even circle, then the line $[1, a]$ of R'_0 intersects only type 0 lines of S'_d if $d \equiv 0 \pmod 4$ and only type 2 lines of S'_d if $d \equiv 2 \pmod 4$.*

Proof. Since $q \equiv 3 \pmod 4$, $q+1$ is divisible by 4. By Lemma 2.2, if $1+\delta^s = \theta^t$, then $s+t \equiv 0 \pmod 4$. It follows that if $(1-h_1)/(1-h_2) = \theta^k$ and $h_1/h_2 = \delta^l$, then $k+l \equiv 0 \pmod 4$. Lemma 4.6 now follows from the proof of Lemma 4.5. □

For the rest of this section, we assume that $q \equiv 3 \pmod 4$ and that $1 + Ha$ is an even circle, where $a \in \mathrm{GF}(q)^*$. Then, the tangent circles are $H(1 + a)$ and $H(1 - a)$. The $(q + 3)$-nest constructed from $1 + Ha$ consists of the reguli $R_0, R_1, R_2, \ldots, R_q$ together with the reguli $[H(1+a), 0]$ and $[H(1-a), 0]$. There is a companion $(q + 3)$-nest consisting of the reguli $S_0, S_1, S_2, \ldots, S_q$ together with the reguli $[H(1 + a), 0]$ and $[H(1 - a), 0]$. The line-set of each of these nests is the same and consists of all lines of the form $[\delta^i + \delta^j a, 0]$ together with the lines of the form $[\delta^i(1 \pm a), 0]$. The regulus $R_i = [\delta^i + Ha, 0]$ is obtained by taking all the lines for some fixed i, while the regulus $S_j = [\delta^j a + H, 0]$ is obtained by taking all the lines for some fixed j. The lines in the opposite reguli $R'_0, R'_1, R'_2, \ldots, R'_q$ and $S'_0, S'_1, S'_2, \ldots, S'_q$ consist of all lines either of the form $[\delta^i, \delta^j a]$ or of the form $[\delta^i a, \delta^j]$.

Consider the following property that an even circle $1 + Ha$ may satisfy:

($\star$) the line $[1, a]$ of R'_0 intersects only lines of type 0 of R'_d if $d \equiv 2 \pmod 4$ and intersects only lines of type 2 if $d \equiv 0 \pmod 4$ for $d \neq 0$.

Lemma 4.7. *Assume that $q \equiv 3 \pmod 4$ and that $1 + Ha$ is an even circle, where $a \in \mathrm{GF}(q)$. Then, $1 + Ha$ satisfies property ($\star$) if and only if $1 + \delta^{2i}a$ is a nonsquare of $\mathrm{GF}(q^2)^*$ for $i = 1, 2, \ldots, \frac{q-3}{4}$.*

Proof. Since $a \in \mathrm{GF}(q)$, the conjugate pairs of elements in Ha are $a\delta^i$, $a\delta^{-i}$ for $i = 1, 2, \ldots, (q - 1)/2$ with $a\delta^{(q+1)/2} = -a \in \mathrm{GF}(q)$. Suppose that $1 + \delta^i a = \delta^d(1 + \delta^{-i})$. By Lemma 4.2, the line $[1, a]$ of R'_0 intersects the line $[\delta^d, \delta^{d-2i}a]$ of R'_d and the line $[\delta^{-d}, \delta^{-(d-2i)}a]$ of R'_{-d}. Thus, $1 + Ha$ satisfies property ($\star$) if and only if i is odd whenever d is even. As in the proof of Lemma 3.1(d), d is even if and only if $1 + \delta^i a$ is a square of $\mathrm{GF}(q^2)$. The result follows. □

Lemma 4.8. *Assume that $q \equiv 3 \pmod 4$ and that $1 + Ha$ is an even circle satisfying property ($\star$). Then, $1 + Ha^{-1}$ satisfies property ($\star$).*

Proof. Since $1 + Ha$ is even, we may assume that $a \in \mathrm{GF}(q)$. Then, of course, $a^{-1} \in \mathrm{GF}(q)$. Since $1+\delta^{2i}a = \delta^{2i}a(1+\delta^{-2i}a^{-1})$, $1+\delta^{2i}a$ is a nonsquare of $\mathrm{GF}(q^2)^*$ if and only if $1+\delta^{-2i}a^{-1}$ is a nonsquare of $\mathrm{GF}(q^2)^*$. The result now follows from Lemma 4.7. □

Theorem 4.9. *Assume that $q \equiv 3 \pmod 4$ and that $1 + Ha$ is an even circle satisfying property ($\star$). Then, each of the following sets of lines is a replacement set for the $(q + 3)$-nest constructed from $1 + Ha$:*

($\mathcal{L}_1$) *lines either of the form $[\delta^i, \delta^j a]$, i even, $i + j \equiv 0, 1 \pmod 4$ or of the form $[\delta^i a, \delta^j]$, i even, $i + j \equiv 2, 3 \pmod 4$, together with the lines $[\delta^i(1 \pm a), 0]$, i odd;*

($\mathcal{L}_2$) *lines either of the form $[\delta^i, \delta^j a]$, j even, $i + j \equiv 0, 1 \pmod 4$ or of the form $[\delta^i a, \delta^j]$, j even, $i + j \equiv 2, 3 \pmod 4$, together with the lines $[0, \delta^j(1 \pm a)]$, j odd.*

Proof. The lines of type $[\delta^i, \delta^j a]$ in either partial spread are pairwise skew since $1 + Ha$ satisfies property $(\star)$. The lines of type $[\delta^i a, \delta^j]$ are pairwise skew since $1 + Ha^{-1}$ satisfies property $(\star)$. Any line of the first type is skew to a line of the second type by Lemma 4.6.

The line $[\delta^i, \delta^j a]$ of R'_i contains a unique point of the hyperbolic quadric $\mathcal{Q}$ determined by the regulus $[H(1+a), 0]$ (or its opposite $[0, H(1+a)]$). Since $[\delta^i, \delta^j a]$ intersects both $[\delta^i(1+a), 0]$ and $[0, \delta^j(1+a)]$, the point of $[\delta^i, \delta^j a]$ on $\mathcal{Q}$ is the point of intersection of $[\delta^i(1+a), 0]$ and $[0, \delta^j(1+a)]$. Similarly, the unique point of $\mathcal{Q}$ on the line $[\delta^i a, \delta^j]$ of S'_i is the point of intersection of $[\delta^i(1+a), 0]$ and $[0, \delta^j(1+a)]$. Thus, the lines of $\mathcal{L}_1$ of the form $[\delta^i, \delta^j a]$ and $[\delta^i a, \delta^j]$ do not intersect any of the lines $[\delta^i(1+a), 0]$ with i odd. A similar argument shows that they do not intersect any of the lines $[\delta^i(1-a), 0]$ with i odd. Thus, the lines of $\mathcal{L}_1$ are pairwise skew. The lines of $\mathcal{L}_2$ of the form $[\delta^i, \delta^j a]$ and $[\delta^i a, \delta^j]$ do not intersect any of the lines $[0, \delta^j(1+a)]$ with j odd, nor any of the lines $[0, \delta^j(1-a)]$ with j odd. Thus, the lines of $\mathcal{L}_2$ are pairwise skew. In each case, we have $(q+3)$ pairwise skew lines which cover only points covered by lines of the $(q+3)$-nest. Thus, they form a replacement set. □

Remarks. (a) The partial spread $\mathcal{L}_1$ is a union of half-reguli of R'_d and S'_d for d even, together with half-reguli of $[H(1 \pm a), 0]$. The partial spread $\mathcal{L}_2$ is a union of quarter-reguli in each R'_d and S'_d, together with half-reguli of the opposite reguli $[0, H(1 \pm a)]$. None of the lines of $\mathcal{L}_2$ is a line of the $(q+3)$-nest, whereas the lines of $[H(1 \pm a), 0]$ in $\mathcal{L}_1$ are lines of the $(q+3)$-nest.

(b) In the definitions of $\mathcal{L}_1$ and $\mathcal{L}_2$, we could replace the requirement that i or j is even by the requirement that i or j is odd. In addition, we could replace the partition $\{0,1\} \cup \{2,3\}$ of values mod 4 in the congruences: $\{0,1\} \cup \{2,3\} \mapsto \{1,2\} \cup \{0,3\} \mapsto \{2,3\} \cup \{0,1\} \mapsto \{0,3\} \cup \{1,2\}$. Thus, for each type, we have 8 cases.

We now consider two interesting examples, where the hypotheses of Theorem 4.9 hold.

Theorem 4.10. *Assume* $q = 7$. *Let* θ *be a primitive element of* GF(7^2) *satisfying* $\theta^2 + \theta + 3 = 0$ *over* GF(7). *Then, the* 10*-nest of* PG(3, 7) *constructed from* $1 + H\theta^2$ *is replaceable, as in Theorem* 4.9.

Proof. The Jacobi logarithm for GF(7^2) (with respect to θ) is listed in the following table. The entry in each cell is the value of j given by $1 + \theta^i = \theta^j$, where the cells in the array are labelled by $i = 0, 1, 2, \ldots, 47$, increasing along successive rows (the missing value corresponds to $i = 24$ since $\theta^{24} = -1$).

16	31	35	6	41	1
23	25	32	22	46	26
14	20	5	10	8	28
45	9	19	42	34	4
∗	29	12	21	47	38
27	11	40	43	39	7
2	15	36	13	24	18
17	44	37	3	33	30

The third column of the table corresponds to the circle $1 + H\theta^2$. The coset $H\theta^2 = H\theta^8$, where $a = \theta^8 \in$ GF(7). The entries 32 and 40 in the third column correspond to the elements $1 \pm a$ of GF(7). We have $1 + \delta^2 a = 1 + \theta^{20} = \theta^{19}$ which is a nonsquare of GF(49)*. Thus, by Lemma 4.7, $1 + H\theta^2$ satisfies property $(\star)$. Hence, the theorem follows from Theorem 4.9. □

Theorem 4.11. *Assume* $q = 11$. *Let* θ *be a primitive element of* GF(11^2) *satisfying* $\theta^2 + \theta - 4 = 0$ *over* GF(11). *Then, the* 14*-nest of* PG(3, 11) *constructed from* $1 + H\theta^2$ *is replaceable, as in Theorem* 4.9.

Proof. The Jacobi logarithm for GF(11^2) (with respect to θ) is listed in the following table.

36	71	66	30	58	18	62	95	11	43
59	61	108	111	40	19	31	86	115	29
94	14	6	21	84	17	77	119	53	105
93	110	33	90	80	67	48	42	47	2
20	116	107	8	38	89	7	102	72	117
91	73	35	39	16	78	101	109	37	87
$*$	28	99	52	45	23	82	106	103	22
41	68	24	55	81	44	114	85	65	75
100	83	9	5	12	32	46	57	1	79
63	76	25	92	51	112	60	118	104	113
74	10	97	69	15	4	26	98	96	50
49	34	3	88	56	13	54	27	64	70

The third column of the table corresponds to the circle $1 + H\theta^2$. The coset $H\theta^2 = H\theta^{12}$, where $a = \theta^{12} \in \mathrm{GF}(11)$. The entries 108 and 24 in the third column correspond to the elements $1 \pm a$ of GF(11). Both $1 + \delta^2 a = 1 + \theta^{32} = \theta^{33}$ and $1 + \delta^4 a = 1 + \theta^{52} = \theta^{35}$ are nonsquares of GF$(11^2)^*$. Thus, by Lemma 4.7, $1 + H\theta^2$ satisfies property $(\star)$. Hence, the theorem follows from Theorem 4.9. □

Concluding remarks. If $q = 11$ and θ is the primitive element specified in Theorem 4.11, then $1 + H\theta^4$ does not satisfy property $(\star)$ since $1 + \theta^{44} = \theta^{38}$ is a square (for this column $a = \theta^{24}$ and $1 + a = \theta^{84}$ so the critical entries are 38 and 45). By Lemma 4.8, neither does $1 + H\theta^6$. The author has verified that no even circle $1 + Ha$ satisfies property $(\star)$ for $q = 19$, $q = 23$ and $q = 31$. This may be the case for all $q \geqslant 19$ and $q \equiv 3 \pmod 4$ since the cyclotomic condition given in Lemma 4.7 is very restrictive.

The author has verified, by computation, that there is no replacement set consisting of a union of opposite half-reguli for the replaceable nests of Theorems 4.10 and 4.11. As mentioned in the Introduction, this is very interesting as they are the first known examples of replaceable nests with this property.

References

[1] R.D. Baker, G.L. Ebert, A new class of translation planes, Ann. Discrete Math. 37 (1988) 7–20.
[2] R.D. Baker, G.L. Ebert, Filling the nest gaps, Finite Fields Appl. 2 (1996) 42–61.
[3] R.H. Bruck, Construction problems of finite projective planes, in: Proc. Conf. Combinatorial Mathematics, Univ. of North Carolina Press, Chapel Hill, 1969, pp. 426–514.
[4] A.A. Bruen, Inversive geometry and some translation planes, I, Geom. Dedicata 7 (1978) 81–98.
[5] P. Dembowski, Finite Geometry, Springer-Verlag, Berlin, Heidelberg, 1997.
[6] G.L. Ebert, Nests, covers and translation planes, Ars Combin. 25c (1988) 213–233.
[7] G.L. Ebert, Spreads admitting regular elliptic covers, European J. Combin. 10 (1989) 319–330.
[8] O. Heden, Maximal partial spreads and the n-queen problem, Discrete Math. 120 (1993) 75–91.
[9] O. Heden, On Bruen chains, Discrete Math. 146 (1995) 69–96.
[10] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Addison–Wesley, Reading, MA, 1983.
[11] H.H. Mitchell, On the congruence $cx^\lambda + 1 = dy^\lambda$ in a Galois field, Ann. of Math. 2 (1916–1917) 120–131.
[12] R.A. Weida, An extension of Bruen chains, Geom. Dedicata 30 (1989) 11–21.